UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/885,234	06/19/2001	Christopher J. Cormack	42390.P11396	4422

8791 7590 04/10/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 04/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/885,234	CORMACK ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2001*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,10-15,19-24 and 29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6, 10-15, 19-24 and 29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on January 13, 2006. Independent claims 16 and 25 have been canceled and dependent claims 7-9, 17-18, 26-28 and 30 have been canceled too. The rest of the Independent claims **1, 10, 19** have been amended. Therefore claims **1-6, 10-15, 19-24 and 29** are pending and are examined.

Response to Arguments

2. Applicant's arguments with respect to **claims 1-6, 10-15, 19-24 and 29** have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 5 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 5 is indefinite because it recites "**authenticating the system registry after reading the system registry**" which is not found in the claim 1 from which it currently is dependent. Examiner interpreted the limitation "**authenticating the system registry after reading the system registry**" as

"**authenticating by the application program the system registry after reading the system registry**" to avoid ambiguity.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-6, 10-15,19-24 and 29** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kathrow et al**. (hereinafter referred as **Kathrow**)(U.S. Patent No. 6,263,348) in view of **Pereira**. (hereinafter referred as Pereira)(U.S. Patent No. 5, 809, 230)

7. **As per claims 1-2,10-11 and 29** **Kathrow** discloses a method to detect tampering with registry settings in a computer comprising:

- **Generating a user identity value [hash Value of the user Password] associated with a user identity**; (In Microsoft operating system, in the process of authentication, generation of a user identity value or the hash value of the user password is inherently included. For NT, user enters their password and the clients hashes the user's password, and generates the hash value or the user identity value and encrypts the server's challenge with this hash and sends two responses to the server: One response uses the LAN Manager hash and

another response uses the stronger NT hash. The server then compares the client's response hash with the client's hash in the SAM Registry hive.)(For the source/explanation that the examiner used, see reference U, page 2, second paragraph)

- **Storing the user identity value [hash value of the user password]**; (Storing the **client's hash** or **the user identity value** or **the hash value of the user password**, in the SAM Registry as explained above for the purpose of authentication is inherently included in the Microsoft operating system, NT) (For the explanation/source that the examiner used See reference U, page 2, second paragraph)

Furthermore **Kathrow** discloses

- **Generating a registry security value [Fingerprint of the registry file/s which includes hash value of the Windows registry file/s] associated with a system registry**; [column 5, lines 11-25; column 4, lines 26-column 5, line 25; figure 2, ref. Num "222" and "232"]

- **Storing the registry security value**; [Column 5, lines 11-26; figure 2, ref. Num "232"] (content storage stores the fingerprint of the file shown on figure 2, ref. Num "232") and

- **Authenticating by the application program the system registry after reading the system registry**.(As explained in the disclosure and on the dependent claim 5, this limitation **comprises**

- **Generating a new registry security value [Fingerprint of the registry file/s which includes hash value of the Windows registry file/s]**; [Column 5, lines 41-62; figure 2, ref. Num "234"] (The new registry finger

print is generated and stored on storage shown on figure 2, ref. Num "234"]

- **Comparing the new registry security value with the stored registry security value**; [Column 6, lines 20-21; column 7, lines 1-6; figure 2, ref. Num "242"] and **allowing processing to continue if the new registry security value is equal to the stored registry security value**.[Column 6, lines 32-36; column 10, lines 38-43] (The processing will not be allowed to continue if the new registry security value is not equal with the stored security value. If this is the case, that is if they are found to be different, then the comparison result will be reported.)

Kathrow does not explicitly disclose

A user identity value associated with a user identity authorized to change a system registry of the computer is generated by an application program running in the computer and

The generated registry security value which associated with system registry is generated by the application program.

However, in the field of endeavor **Pereira**, discloses

The access control program may use an application program interface (API) to modify the registry system file in accordance with the restricted list files generated by the access control program. [Column 10, lines 29-33 and column 10, line 1-column 11, line 10]. This meets the limitation of A user identity value associated with a user identity authorized to change a system registry of the computer is generated by an application program running in the computer and the generated registry security value which associated with system registry is generated by the application program.

Furthermore **Pereira** discloses detecting an attempt to change a system registry;[column 4, lines 49-54; column 4, lines 40-44; column 4, lines 49-51 column 10, lines 20-21] and generating a user identity value associated with the user identity;[column 10, lines 20-26] (if the user enters the corresponding password user would be able to define/access resources in the registry)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of a user identity value associated with a user identity authorized to change a system registry of the computer is generated by an application program running in the computer and the feature of generating registry security value which associated with system registry by application program as per teachings of **Pereira** into the method taught by **Kathrow**, in order to provide more security to prevent tampering with registry settings.[**See Pereira**, column 4, lines 49-54; column 4, lines 40-44; column 4, lines 49-51 column 10, lines 20-21]

8. **As per claims 19-20** **Kathrow** discloses an Apparatus **comprising**:

- **A bus**; [figure 1] (The bus is inherently included in the computer system shown on figure 1, it connects the cpu/processor with the memory or storage)

- **A data Storage device coupled to said bus and that stores a plurality of instructions which implement an application program**;[Figure 1, ref. Num "162" and "164" and column 3, lines 23-34) (The storage device shown on figure 1, ref. Num "162 and "164" are coupled to the processor by said bus as shown on figure 1 and also software instructions are stored in storage 162 as explained on column 3, lines 23]

- **A processor coupled to said data storage device**, [figure 1, ref. Num "160" and "162" and "164")

- **Said processor operable to receive said instructions which, when executed by the processor, cause the processor to [Column 3, lines 23-27; column 3, lines 27-56]**

- **Generating a user identity value [hash Value of the user Password] associated with a user identity**; (In Microsoft operating system, in the process of authentication, generation of a user identity value or the hash value of the user password is inherently included. For NT, user enters their password and the clients hashes the user's password, and generates the hash value or user identity value and encrypts the server's challenge with this hash and sends two responses to the server: One response uses the LAN Manager hash and another response uses the stronger NT hash. The server then compares the client's response hash with the client's hash in the SAM Registry hive.)(For the explanation/source that the examiner used, see reference U, page 2, second paragraph)

- **Storing the user identity value [hash value of the user password]**; (Storing the **client's hash** or **the user identity value** or **the hash value of the user password**, in the SAM Registry as explained above for the purpose of authentication is inherently included in the Microsoft operating system, NT) (For the explanation/source that the examiner used See reference U, page 2, second paragraph)

Furthermore **Kathrow** discloses

- **Generating a registry security value [Fingerprint of the registry file/s which includes hash value of the Windows registry file/s]**

associated with a system registry; [Column 5, lines 11-25; column 4, lines 26-column 5, line 25; figure 2, ref. Num "222", ref. Num "232"]

- **Storing the registry security value**; [Column 5, lines 11-26; figure 2, ref. Num "232"] (content storage stores the fingerprint of the file shown on figure 2, ref. Num "232") and

- **Authenticating the system registry after reading the system registry based on the stored registry security value**.(As explained in the disclosure and on the dependent claim 5 and 23, this limitation **comprises**

- **Generating a new registry security value [Fingerprint of the registry file/s which includes hash value of the Windows registry file/s]**; [Column 5, lines 41-62; figure 2, ref. Num "234"] (The new registry finger print is generated and stored on storage shown on figure 2, ref. Num "234"]

- **Comparing the new registry security value with the stored registry security value**; [Column 6, lines 20-21; column 7, lines 1-6; figure 2, ref. Num "242"] and **allowing processing to continue if the new registry security value is equal to the stored registry security value**.[Column 6, lines 32-36; column 10, lines 38-43] (The processing will not be allowed to continue if the new registry security value is not equal with the stored security value. If this is the case, that is if they are found to be different, then the comparison result will be reported.)

Kathrow does not explicitly disclose

Generating a user identity value associated with a user identity authorized to change a system registry of the said apparatus

However, in the field of endeavor **Pereira**, discloses

The access control program may use an application program interface (API) to modify the registry system file in accordance with the restricted list files generated by the access control program.[Column 10, lines 29-33 and column 10, line 1-column 11, line 10]. This meets the limitation of a user identity value associated with a user identity authorized to change a system registry of the computer is generated by an application program running in the computer and the generated registry security value which associated with system registry is generated by the application program.

Furthermore **Pereira** discloses detecting an attempt to change a system registry;[column 4, lines 49-54; column 4, lines 40-44; column 4, lines 49-51 column 10, lines 20-21] and generating a user identity value associated with the user identity;[column 10, lines 20-26] (if the user enters the corresponding password user would be able to define/access resources in the registry)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of a user identity value associated with a user identity authorized to change a system registry of the computer is generated by an application program running in the computer and the feature of generating registry security value which associated with system registry by application program as per teachings of **Pereira** into the method taught by **Kathrow**, in order to provide more security to prevent tampering with

registry settings.[**See Pereira**, column 4, lines 49-54; column 4, lines 40-44; column 4, lines 49-51 column 10, lines 20-21]

9. **As per claims 3-4 and 12-13 the combination of Kathrow and Pereira** discloses a method as applied to claims 1 and claim 10 above. Furthermore **Kathrow discloses the method wherein** generating a registry security value associated with a system registry comprises: concatenating system registry information; and inserting the concatenated system registry information in a one-way function to obtain the registry security value. [Column 4, lines 26-column 5, line 25; figure 2, ref. Num "232"]

10. **As per claims 5-6 and 14-15 the combination of Kathrow and Pereira** discloses a method as applied to claims 1 and 10 above. Furthermore **Kathrow discloses the method wherein authenticating the system registry after reading the system registry comprises:**

- **Generating a new registry security value [Fingerprint of the registry file/s which includes hash value of the Windows registry file/s]**; [Column 5, lines 41-62; figure 2, ref. Num "234"] (The new registry finger print is generated and stored on storage shown on figure 2, ref. Num "234"]

- **Comparing the new registry security value with the stored registry security value**; [Column 6, lines 20-21; column 7, lines 1-6; figure 2, ref. Num "242"] and **allowing processing to continue if the new registry security value is equal to the stored registry security value**.[Column 6, lines 32-36; column 10, lines 38-43] (The processing will not be allowed to continue if the new registry security value is not equal with the stored security value. If this is the case, that is if they are found to be different, then the comparison result will be reported.)

11. **As per claims 21-22** **the combination of Kathrow and Pereira** discloses an apparatus as applied to claim 19 above. Furthermore **Kathrow discloses an apparatus** wherein the processor operable to receive instructions which, when executed by the processor, cause the processor to generate a registry security value associated with a system registry comprises the processor to concatenate system registry information; and to insert the concatenated system registry information in a function to obtain the registry security value. [Column 4, lines 26-column 5, line 25; figure 2, ref. Num "232"]

12. **As per claims 23-24** **the combination of Kathrow and Pereira** discloses an apparatus as applied to claim 19 above. Furthermore **Kathrow discloses an apparatus** wherein the processor operable to receive instructions which, when executed by the processor, cause the processor to **authenticate the system registry after reading the system registry comprises the process :**

- **Generating a new registry security value [Fingerprint of the registry file/s which includes hash value of the Windows registry file/s]**; [Column 5, lines 41-62; figure 2, ref. Num "234"] (The new registry finger print is generated and stored on storage shown on figure 2, ref. Num "234"]

- **Comparing the new registry security value with the stored registry security value**; [Column 6, lines 20-21; column 7, lines 1-6; figure 2, ref. Num "242"] and **allowing processing to continue if the new registry security value is equal to the stored registry security value**.[Column 6, lines 32-36; column 10, lines 38-43] (The processing will not be allowed to continue if the new registry security value is not equal with the stored security value. If this is the case, that is if they are found to be different, then the comparison result will be reported.)

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.

March 25, 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100